

行動科学から見た

解説

情報セキュリティとプライバシー
に関する研究についてSome Examples of Information Security and Privacy Issues
from the View Point of Behavioural Science

上田昌史

Abstract

ネットワークを利用したサービスが普及し、社会生活や経済活動にも大きく影響を与えるようになってきた。そこで、利用者のセキュリティやプライバシーに関する態度の変容や利用行動の構造を明らかにするために、行動科学的なアプローチが必要となってきた。本稿ではこのような課題に対して「情報セキュリティ対策に関する調査」と「プライバシーに関する調査」を取り上げ、その調査の中で利用者による行動がどのような構造を持っているかを様々なアプローチで説明しようとする試みを紹介する。

キーワード：情報セキュリティ、プライバシー、ロボット、行動科学

1. はじめに

近年、センサ類やスマートフォン等の普及に加えてビッグデータの分析が行われてきたため、リアルとネットの融合サービスが増え、ネットワークを利用したサービスが日常生活に浸透し、社会生活や経済活動にも大きく影響を与えるようになってきた。特に、日常生活で普通に使うサービスの中でも、「プラスチックカード」あるいは「携帯電話に内蔵されたICカード」の中に「ある特定の識別情報（ID）」をひも付けすることで、各主体の行動履歴をより詳しく分析した結果を用いて、利便性が向上したサービスが頻繁に見られるようになった（表1）⁽²⁾。

一方、交通系ICカードを利用して支払うと、「どのような手段で移動し、どの店舗で何を幾らでどのような方法で買ったか」といったプライバシーに関わる情報を提供することになる。利用契約の内容にもよるが、この購入履歴や利用履歴といった利用者情報がサービス提供者や許可された第三者に蓄積、分析される場合がある。

本稿はNextcom 8号の原稿⁽¹⁾をベースに書き改めたものである。

上田昌史 京都産業大学経済学部経済学科
E-mail masashi.ueda@cc.kyoto-su.ac.jp
Masashi UEDA, Nonmember (Faculty of Economics, Kyoto Sangyo University,
Kyoto-shi, 603-8555 Japan).
電子情報通信学会誌 Vol.96 No.8 pp.656-661 2013年8月
©電子情報通信学会 2013

表1 国内における主要8種の電子マネーの動向（出典：文献（2）から著者作成）

	発行枚数 (万枚)	端末台数 (万台)	決済件数 (百万件)	決済金額 (億円)
2007年9月	6,649	25	72	483
12月	7,326	29	75	599
2008年3月	8,061	36	81	582
6月	8,761	38	87	657
9月	9,308	39	94	635
12月	9,885	45	97	777
2009年3月	10,503	48	103	771
6月	11,321	52	119	927
9月	11,850	56	124	993
12月	12,426	59	132	1,217
2010年3月	12,989	67	143	1,180
6月	13,715	77	168	1,393
9月	14,156	80	170	1,418
12月	14,647	84	169	1,571
2011年3月	15,174	89	161	1,417
6月	15,852	96	194	1,637
9月	16,453	99	199	1,652
12月	16,975	103	201	1,946
2012年3月	17,497	107	204	1,774
6月	18,217	112	228	1,981

（注）PiTaPaやiDのような後払（ポストペイド）方式やちょコムeマネーのようにサーバに価値を保存する方式もあるが、この表では、前払（プリペイド）方式の專業系（楽天Edy）、交通系（Suica, ICOCA, PASMO, SUGOCA, Kitaca）、及び流通系（nanaco, WAON）の8種類を対象としている。

サービス提供者等は、この利用者に関わる情報を活用して、ポイントやマイレージなどの付与や、お買い得情報やおすすめ情報の提供を行う。これにより利用者は、経済性や利便性などが向上するサービスを楽しむことができる。このような仕組みを利用した極端な例では、日常生活の消費に際して、支払手段や店選びを「特定の航空会社のマイル」が最もたまるように設計している「マイラー（＝航空会社のマイルを必死になってためている人）」と呼ばれるような利用者さえもいる。

経済学では、このようなサービス提供事業者と顧客の関係を「囲い込み（Lock in）」^(注1)、⁽³⁾と呼んでいる。楽しみながらお互いにメリットがあって囲い込まれるのであれば、何ら問題ない。しかし、囲い込みから容易に抜け出せなくなったり、知らぬ間に、サービス提供事業者等によって、このような利用者情報が蓄積され、利用されたりすることに漠然とした不安感がある利用者も少なく存在するであろう。

もちろん、良心的なサービス提供事業者は、このような状況を理解して、サービスの設計を行っている。また、安全の提供のために、暗号化技術の高度化や秘密分散法などのような技術的な方法論も検討されている。しかし、理論的には安全であっても、利用者が安心して使えなければ、心理的なハードルを超える説得力は持たないだろう。

そこで、工学的な安全性を高める方法に加えて社会科

学的な分析、特に、行動科学的なアプローチが必要となってきた。すなわち、まず、利用者がサービス利用に至るまでのプロセスにおいて、利用者のセキュリティやプライバシーに関する態度の変容や利用行動の構造を明らかにする必要がある。

その構造を理解することで、利用者に過度に心理的負担をかけない方法で、ネットワーク化された状況下での利用者情報を活用する仕組みを検討できる。本稿では、二つの調査研究を基にこのテーマに関してのアプローチを紹介する。

2. 情報セキュリティ対策に関する調査

まずは、筆者も2007年から参加していた独立行政法人情報処理推進機構（IPA）情報セキュリティ分析ラボラトリーで行われた情報セキュリティ対策に関わる調査を、文献（4）及び（5）を参考にしながら紹介する。

この調査では、総務省と経済産業省及び業界が協力して設立されたサイバークリーンセンター（CCC）^(注2)は、コンピュータウイルスの一種であるボット^(用語)を駆除するプログラムを無償で配布しているが、ボットに感染したユーザが、このサイバークリーンセンターが行っている「ボット対策事業」に対して、余り協力的でない（実施率32.5%^(注3)）理由がどこにあるのかを解明することで、日本における情報セキュリティレベルの改善を目指していた。

IPAによるこの一連の調査では、まず、調査の前提として事前には構造が分からないので代表的な理論の幾つかから仮説を立て、それを実験で検証するという手順を取っている。なお、行動経済学では、プロスペクト理論をよく用いるが、本稿では取り扱わない。

2.1 ゲーム理論

ゲーム理論（Game Theory）は、数学者のフォン・ノイマンと経済学者のモルゲンシュテルンによる数学理論から始まる。ミクロ経済学に導入されてからは、二者間の問題を解くツールとして応用され、利害の必ずしも一致しない状況において、意思決定問題や配分問題を探索する方法論の一つとして用いられることがある。ボット対応策を適用しようとする、ゲーム理論の古典的な類型の一つである「共有地の悲劇」^(用語)あるいは「社会的ジレンマ」^(用語)の状況になっている可能性がある。

（注1） 文献（2）によると、日本人はポイントを集めたがる傾向が強い。このような傾向がある集団に対しては、顧客プログラムによる囲い込みは有効である。

■ 用語解説

ボット サイバークリーンセンターの解説によると、「コンピュータを悪用することを目的に作られたプログラムで、コンピュータに感染すると、インターネットを通じて悪意を持った第三者が、あなたのコンピュータを外部から遠隔操作することを目的として作成された悪性プログラム」としている。

共有地の悲劇 The Tragedy of the Commons. 多数の主体が利用可能な共有資源は、各主体が好き勝手に使うと資源の枯渇を招いてしまうという現象。ギャレット・ハーディン（Garrett Hardin）の1968年の論文「The Tragedy of the Commons」（サイエンス）により一般に広く認知されるようになった。

社会的ジレンマ Social Dilemma. 社会において、個人の合理的な選択が、社会としての最適な選択に一致せずかい離が生ずること。ごみや環境に関する問題においてしばしば指摘される。

コンジョイント分析 Conjoint Analysis. 1980年代にマーケティング分野で開発された調査法で実験計画法の応用。商品やサービスが持つ複数の要素について、利用者や消費者がどの要素を重視しているか、あるいはどのような組合せが好まれるかを統計的に調査することができる。

（注2） 詳しくはサイバークリーンセンター（<https://www.ccc.go.jp/>）のホームページを参照。なお、CCCは2011年に組織変更を行っている。
（注3） ボット感染が検知された利用者に対して、インターネットサービスプロバイダ経由で、ボット感染の警告と駆除ツール（プログラム）の導入を呼びかけるメールを送付した際、実際にCCCから駆除ツールをダウンロードした比率。詳細はCCCのホームページを参照。
<https://www.ccc.go.jp/report/201012/1012monthly.html>

すなわち、ボットに感染した人がみんな、手間を惜しまず、ボット駆除ツールを導入するとインターネットはより安全になるはずであるが、各個人にとっては手間がかかるだけの作業であり実際には実施されない、といった仮説が成り立つ可能性がある。

2.2 防護動機理論

説得心理学の分野で、危機感を喚起する理論の一つであるロジャースの修正防護動機理論 (PMT: Protection Motivation Theory)^{(6), (7)}では、個人の態度変容は、危機感を喚起するために与えられたメッセージの内容から、「事態の深刻さ」、「事態の生じる確率 (生起確率)」、「事態に対応する費用」などが情報の受け手の防護動機を決定し、「対処行動の効果」、「自己の能力」などが対処評価を決定すると仮定している。

すなわち、ボット駆除ツールをインストールするよう注意する電子メールの文面がどのように書かれるかによってその効果に差が見られる可能性がある。

2.3 精緻化見込みモデル

同じく説得心理学の分野の理論であるが、説得メッセージを与えられたときに、個人が情報を処理し態度変容する際に、ルートが2種類あるというのが精緻化見込みモデル (ELM: Elaborative Likelihood Model)⁽⁸⁾である。精緻化見込みモデルでは、説得メッセージを与えられたときの人々の反応は、「中心ルート」と「周辺ルート」の二つに分かれるというものである。

説得メッセージの内容を吟味し理解して、論理的に行動する「中心ルート」、理解力の不足から内容そのものとは直接関係しない要因に影響される「周辺ルート」で

ある。

すなわち、ボット駆除ツールのインストール行動には各個人の知識、経験、あるいは日頃の行動様式に影響される可能性がある。

これらを参考にしながら、2010年春にボット感染の通知メールがISPから送られてくる状況をインターネット調査で再現して質問した。その質問の順序は図1に整理している。なお、年代、男女別に均等割り付けを行い、有効サンプル数は5,136であった。

この調査から次のような結果が導き出された。

(1) 社会的ジレンマは起きていない。

まず、各個人にとってボット駆除による効果は駆除ツール導入の手間を上回っており、共有地の悲劇の一種である社会的ジレンマは起きていない。

しかし、手間の削減は効果が見られるので、駆除ツール提供方法や操作性の改善は、協力率向上に有用な方法論であることが分かった。

また、被害の及ぶ範囲と対策の有効性や手間を聞いた質問で類型化したときに、社会的ジレンマの状況は「自分に被害が及ばず、他人に被害が及ぶ。対策の効果は有効ではなく、手間がかかっている」とであるが、この類型に当てはまる回答者は僅か1.0%であり、社会的ジレンマの状況ではない。

(2) フリーライダーが多いわけではなかった。

メールに書かれたメッセージの理解度が高まると駆除ツール導入の確率も高まっており、「みんなが対策を取れば、自身は対策しなくても比較的 안전한 インターネット環境を享受できる」と考えるフリーライダー (ただ乗り) は観測されなかった。

メールに書かれたメッセージの理解度を高めると協力してくれる可能性が高まる (中心ルートを選択する人が増える) ので、状況を内容分かりやすく簡潔に伝えるメールの文面の工夫が必要であることが分かる。

(3) 認知順序は身近なところから。

今回のような状況で個人が状況を理解していく順序は、自分に被害が及ぶ、他人に被害が及ぶ、対策の効果が有効である、対策の手間は大了たことがないの順であった。

ここから分かるのは、メールの文面で、「他人事ではない」と感じてもらう説得が必要であるということである。自己危機感を持てば、67.1%は協力する意向を示しているの、大変有効であると言える。

この調査結果を信頼するならば、多くの人は利己的であるからボット対処策をしないわけではないので、より多くのボット感染者に駆除ツールを導入してもらうため

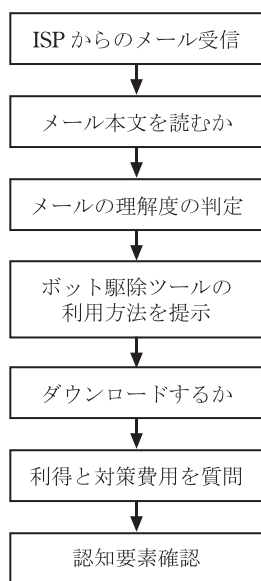


図1 質問の順序 (出典: 文献(3)から筆者修正)

には、以下に示す対策が効果的であることが分かる。

- ・ボットに関して、適切に理解し行動をしてもらうために、分かりやすい文章で警告を行うとともに、一般的な啓発活動が必要である（中心ルートへ誘導）。
- ・ボット感染を放置すると自分にも危害が及ぶ可能性があることを理解してもらう（自己危機感の醸成）。
- ・より協力しやすいように、ボット駆除の手間を減らす（非費用感の向上）。

3. プライバシーに関する調査

ここからは、利用者の「態度や行動」をどのように観察し分析し解明するかを、同じく IPA の情報セキュリティ分析ラボラトリーで行われた eID に関する調査及び研究^(注4)、⁽⁹⁾ 及び、そのアイデアの基になった欧州での調査を用いて紹介する。ここでいう eID とは情報システムで用いられる ID (Identity) で、ユーザの識別子 (Identifier) に加えて、その識別子の付属する属性情報を含むものである。

3.1 欧州での調査

スペインのセビリアにある EU の研究機関 IPTS (Institute for Prospective Technology Studies) は、2008 年夏に「個人情報インターネットなどで提供することに対するヨーロッパ人の認知」に関する調査をインターネット調査^(注5)を用いて行った。イギリス、ドイツ、フランス、スペインの各国に住む 15 歳から 25 歳の若者が対象で、各国約 1,000 サンプルを収集した (表 2)⁽¹⁰⁾。これらのデータを用いて、若者が今後、携帯電話や SNS (Social Networking Service) などに情報を提供していく過程でどのようなプライバシーに関わる問題があるかを調査し、結果を 2009 年に公表^(注6)した。

欧州においてもスマートフォンやそのアプリケーションとしての SNS が普及しつつある現在では、現実性のある質問項目が多い。しかし、調査当時では、携帯電話は、通話以外に SMS (Short Messaging Service) や着信音のダウンロード程度の利用であったことを考える

(注 4) 文献(9)を参照。なお、本調査は高橋郁夫弁護士の強いイニシアティブが発揮されている。

(注 5) 従来から「インターネット利用者は若年男性に偏っている」といった批判が強く、インターネット調査は方法論として信任を得ていなかった。しかし、筆者の 1999 年実施調査でも、電話帳からランダムサンプリングした回答者データより、インターネット懸賞サイト経由でサンプリングした回答者データの方が、国勢調査の分布に近い年齢及び性別分布になっていた。この調査のようにインターネット上での行動を分析する場合、ランダムサンプリングさえできていれば、インターネット調査は方法論としてより問題は少ない。

(注 6) 文献(10)を参照。筆者も IPA 小松文子氏とともに、2010 年春にこの調査の実施者を中心とした IPTS 主催の国際ワークショップにて日欧を比較した討論を行った。

表 2 IPTS 調査のサンプル (出典：文献(10)の p. 27)

		フランス	イギリス	スペイン	ドイツ
サンプル数		2,014	1,258	819	1,174
年齢層	15～18 歳	59%	30%	45%	37%
	19～21 歳	31%	29%	27%	29%
	22～25 歳	10%	41%	28%	34%

と、大胆な調査であったと言える。主要な結果の概要は次の 4 点にまとめられる。

(1) インターネット接続方法と専門知識

一般にインターネットは固定回線を用いて日に数回程度接続しており、携帯電話によるインターネット接続はかなり少ない。

しかし、サービスについては、SNS や写真共有サイトなど、いわゆる Web2.0 と呼ばれていたサービスはよく知られていた。また、eID 技術に対する知識も PIN コードやパスワード、バイオメトリクス (生体認証技術)、電子署名などに関しては半数以上の回答者が知っていたが、RFID (Radio Frequency Identification, 無線タグ) は 20% 未満の認知度であった。

この時点では、最新のサービスを固定系インターネットで利用しているが、概して無線系技術の知識及びその利用は普及途上であると言える。

(2) 個人情報保護

インターネットに対して懐疑的で、個人情報の保護に疑問を抱いており、インターネット上で個人情報を提供すると、迷惑メールが増えたり、ID が窃盗されたりしないか心配している。

サービス提供事業者が各国のデータ保護法を遵守すると eID サービスの利用が促進されると感じている。そのため、個人情報やプライバシーが技術的に守られている保証を示す信頼できる主体によるロゴやラベルのようなものがあればいいと感じており、単に個人情報を自らがコントロールできるような仕組み (自己情報コントロール) だけでは利用が進むとは考えていない。

個人情報の管理に関しては、知人や家族を最も信頼しており、よく知られている会社であればある程度は信頼するが、知らない会社、NPO (Non-Profit Organization)、公的機関に対する信頼は低い。

また、EU のデータ保護指令により守られる権利については、約 3 分の 2 の回答者に知られているが、約 80% の回答者は公的機関がセキュリティとプライバシーを守ってくれないと考えている。

データ保護法制の比較的整っている欧州においても、インターネットはまだ法の秩序によって守られておらず、自分と知人で自らの身を守っていくしかない、と

考えているようである。

(3) 個人情報の提供

オンライン上のサービスを利用するための最低限の個人情報や、SNS を利用するために必要な情報は提供するが、それ以上の情報提供には大きなリスクを感じており空欄にしたり虚偽の情報を入力したりするといった対応をしている。

なお、欧州では氏名、年齢、国籍などの情報は 85% の回答者が提供する意思を示しており、匿名性を好む日本の状況との差があると言えるだろう。

(4) シナリオに基づいた分析

eID の利用に関するシナリオを四つ設定して、それに回答してもらうことで、それぞれのサービスと提供する利用情報（SNS 利用と個人情報、インターネット利用とネット上での行動履歴、ガイドブック情報と実行動履歴、優先入場と生体情報）のバランスを評価する方法を用いて調査した。調査の結果、共通した重視される要因は、プライバシーの保護、個人情報を自らがコントロールできるような仕組み、利用料が無料であることであった。

この調査の結果から、具体的にサービスと提供すべき情報を提示して利用動向を聞くことで、ライフスタイルやプライバシー感覚をある程度推定することが可能であることが分かる。

3.2 日本での調査

2010 年冬の IPA の調査では、IPTS の調査項目を比較検討対象としている。対象は、若年層（1,006 サンプル）と一般（若年層とは別に 1,076 サンプル）の双方の集団のデータを収集している（表 3）。

また、サービス提供のために収集・蓄積される利用者の eID と利用者情報に対して、セキュリティとプライバシーに関するリスクを利用者がどのように認識し受容するかを明確にするための調査も実施している。

その中で、日本では一般的になった電子マネー機能内蔵型 IC カードのシナリオを追加しているのが特徴である。

表 3 IPA 調査のサンプル（出典：文献(8)の p. 29)

		若者サンプル	一般サンプル
サンプル数		1,006	1,076
年齢層	15～18 歳	31.3%	24.1%
	19～21 歳	32.9%	
	22～25 歳	35.8%	
	26～35 歳		25.0%
	36～45 歳		25.0%
	46 歳以上		25.9%

る。主要な結果の概要は以下のとおりである。

(1) プライバシー侵害のリスク認知と対策

日本でもインターネットへの信用は低く、特にプライバシーが侵害されるリスクを懸念している。しかし、オンラインで自己防衛するために具体的な対策を取っていない回答者が多いという結果になった。

この点を欧州の調査と比較すると、欧州の方がリスクに対する認知が高く、また多くの利用者が対策を取っている。

(2) プライバシー情報の自己情報コントロール

eID を使用するシステムの利用を推進する方法としては、欧州と同様、法律などによる保証やロゴやラベルなどであると回答したものが多かった。

しかし、個人情報などのプライバシー情報を自らがコントロールできるような仕組み（自己情報コントロール）や履歴などの記録を得ることは、eID を使用するシステムを利用する上でそれほど役立たない、という結果であった。また、プライバシー情報について責任を持つべき第 1 の主体は、サービス事業者であり、次に本人であると考えていることが分かった。

これは、プライバシー保護に対する自己情報コントロールについて、抵抗感があることを示唆している。eID を利用する上で必要な施策としての順位は同じであったが、欧州の方が個人情報等の管理についての情報、履歴などのログの情報が役立つと回答している。

(3) 「センシティブ情報」と「匿名を好む傾向」

利用者に関わる情報を因子分析した結果、4 因子が抽出された。その中で、インターネット上のサービスへ提供する利用者情報のうち、特に強い抵抗感がある情報（センシティブ情報）には、健康保険番号や自身の写真、クレジットカード番号のような財務情報などがあつた。

また、欧州と比較して名前や写真を提供することに抵抗感があることが分かった。これは日本では名前もセンシティブ情報に近いと考えられており、掲示板や SNS において匿名を好む傾向があるのと整合的な結果である。

(4) プライバシー侵害とその他のメリットの関係

プライバシー侵害への懸念と、経済的な価値やコスト、サービス内容について、その選好順序を分析するために、電子マネー機能内蔵型 IC カードについて利用場面を想定しコンジョイント分析^(用語)を行った。

多くの回答者が利用のために必要な条件は、プライバシー保護であると回答するが、選好順序の分析では、経済的価値やコスト、サービス内容、プライバシーの順序を持つことが分かった。

個人情報保護法への過剰反応によって、個人情報の取扱いが面倒で不便になったとよく言われるが、この選好順序の分析からは、利用者情報を条件によっては提供してもよいと思っている人がかなり存在する可能性を示唆している。

利用者情報の提供に対する代償の支払いを直接聞いたリ、「個人情報」の提供をお願いしたりすると、利用者は身構えてしまい、かなり高額な対価を表明してしまう。しかし、具体的な利用場面（経済性、利便性、娯楽性などを兼ね備えたサービス）を想定すると、利用者情報の値段も変化し得る、言い換えれば、個人情報の取引市場は成立し得るということが分かった。

4. まとめと今後の課題

本稿では、情報セキュリティやプライバシーと社会との関わりに関する問題として情報セキュリティ対策とeIDのプライバシーという二つのテーマに関するIPAの調査研究を取り上げた。そこで利用者による行動がどのような構造を持っているかを様々なアプローチで解明しようとする少し荒削りな試みを紹介した。

情報セキュリティやプライバシーの分野に限らず、「人々の行動の解明」を目的とする研究は、今回紹介したように単純に方法論を外部から導入したり、外国の先端事例をそのまま導入したりできないことを示唆している。

つまり、人々が進んで取り入れたいこと、感覚的に受け入れにくいこと、といった行動の背景にある構造は、それぞれの文化的背景、前後の文脈や状況、取引を行う相手などの要因に依存して決まる可能性が高い。その構造の解明と理解が進むと、利用者にとってもサービス提供事業者等にとってもよりよいサービスの提供機会が生まれるはずである。

よって、今後新しいサービスを提供する際には工学的アプローチによる信頼性確保に加えて、今回紹介したような行動科学的アプローチ等を積極的に取り入れていく

ことで、社会的受容性を高めていく必要があるだろう。

文 献

- (1) 上田昌史, “行動科学から見た情報セキュリティとプライバシー,” Nextcom, vol. 8, pp. 22-30, 2011.
- (2) 日本銀行決済機構局, “最近の電子マネーの動向について(2012年),” BOJ Reports & Research papers, 2012.
http://www.boj.or.jp/research/brp/ron_2012/data/ron121119a.pdf
- (3) K. Atcharyachanvanich, H. Okada, and N. Sonehara, “What keeps online customers repurchasing through the internet?,” ACM Special Interest Group on Electronic Commerce, vol. 6, no. 2, pp. 47-57, 2007.
- (4) 小松文子, 高木大資, 松本 勉, “情報セキュリティ対策における個人の利得と認知構造に関する実証研究,” 情報処理, vol. 51, no. 9, pp. 1711-1725, 2010.
- (5) 小松文子, 高木大資, 吉開範章, 松本 勉, “情報セキュリティ対策を要請する説得メッセージによる態度変容の調査,” 情報処理, vol. 52, no. 9, pp. 2526-2536, 2011.
- (6) R.W. Rogers, “A protection motivation theory of fear appeals and attitude change,” Journal of Psychology, vol. 91, pp. 93-114, 1975.
- (7) 木村堅一, “脅威認知・対処認知と説得: 防護動機理論,” 説得心理学ハンドブック, 深田博巳(編), pp. 374-417, 北大路書房, 2004.
- (8) R.E. Petty and J.T. Cacioppo, “The elaborative likelihood model of persuasion,” Advances in Experimental Social Psychology, vol. 19, pp. 123-205, 1986.
- (9) 独立行政法人情報処理推進機構セキュリティセンター, “eIDに対するセキュリティとプライバシーに関するリスク認知と需要の調査報告,” 2010, http://www.ipa.go.jp/security/economics/report/eid_report_2010.pdf
- (10) W. Lusoli and C. Miltgen, “Young people and emerging digital services: An exploratory survey on motivations, perceptions and acceptance of risks,” JRC Scientific and Technical Reports, 2009, <https://www.eid-stork.eu/dmdocuments/public/JRC50089.pdf>

(平成 25 年 4 月 29 日受付 平成 25 年 5 月 23 日最終受付)



う え だ ま さ し
上田 昌史

1998 京大・経済卒, 2003 同大学院情報学研究科指導認定退学, 関西大ソシオネットワーク戦略研究センター (2003~2005), 国立情報学研究所及び総合研究大学院大学助手/助教 (2006~2012), オーストラリア国立大クロフォード経済政治大学院客員研究員 (2006), 公正取引委員会 (2012~2013) を経て現職。経済学の視点からオープンソースソフトウェア, 情報セキュリティ, 電気通信事業, 電気事業といった社会ネットワークインフラを分析。特に, プラットホーム性のあるネットワーク産業の競争モデルと社会に与える影響について研究している。